Evaluation of Delays PUFs on CMOS 65 nm Technology: ASIC vs FPGA

Zouha Cherif, Jean-Luc Danger, Lilian Bossuet

Evaluation of Delay PUFs on CMOS 65 nm Technology: ASIC vs FPGA

Zouha Cherif Jouini[1,2], Jean-Luc Danger[1], Lilian Bossuet[2]
[1]Institut MINES-TELECOM, TELECOM ParisTech, CNRS LTCI, 46 rue Barrault 75 634 Paris, France.
<{cherif,danger}@telecom-paristech.fr>
[2] Université de Lyon, CNRS, UMR5516, Laboratoire Hubert Curien 42 000 Saint-Etienne, France.
<lilian.bossuet@univ-st-etienne.fr>

***Abstract*—This paper presents a work in progress on the comparison between the performance of two types of Physically Unclonable Functions (PUFs), namely the arbiter and the loop PUFs. The arbiter and the loop PUF are designed on two CMOS-65nm technology platforms: ASIC and FPGA (Xilinx Virtex-5). A mixed PUF design is proposed to allow a fair comparison between the two structures. The principal of the mixed PUF design consists on the use of the same delay chains on both arbiter and loop PUF structures. The comparison analysis reveals that the arbiter PUF structure has the worst performance when compared to the loop PUF, on both platforms. We also observe that the performance for both structures are better when designed on ASIC.**

Keywords: PUF, randomness, steadiness, uniqueness, FPGA, ASIC.

I. Introduction

A Physically Unclonable Function (PUF) is a function which returns a characteristic value of an integrated circuit. This signature can be used for cryptographic applications as authentication and key generation purposes. The silicon PUF outputs a "response" (or ID) which depends on a control word, called the "challenge". Due to the dispersion of the manufacturing process, the response for a given challenge is different between PUFs. There are two main classes of silicon PUFs: the PUFs based on delay comparisons, composed of identical elements, and the PUFs exploiting the initial state of memory blocks.

This paper deals with PUFs based on delay chain comparison as arbiter PUF [1] and loop PUF [2].

To perform an efficient characterization of PUFs, at least three metrics are necessary: randomness, uniqueness and steadiness. **The randomness** gives an estimate of the imbalance between the number of IDs at '0' and the IDs at '1' for all the challenges. **The uniqueness** indicates the entropy between two PUFs, either in the same device (intra-uniqueness) or between devices (inter-uniqueness). **The steadiness** expresses the level of PUF reliability which is reduced by the noise coming from the measurement environment.

In this paper we present the intra-device evaluation results of two structures of delay PUFs. The arbiter PUF and the loop PUF are designed on two platforms ASIC and FPGA with a CMOS 65nm technology.

II. Background

A. *Arbiter PUF*

The example structure of the arbiter PUF is made up of M identical delay elements structured as a mini crossbar 2x2, as illustrated in Figure 1. To be sure that the delay difference takes advantage only from CMOS variation, hard routing constraints are needed to make two identical cross coupled delay lines. As proposed by Majzoobi in [3], the arbiter PUF can be designed using two identical parallel delay chains of M elements (Figure 2) in order to reduce the routing constraints.

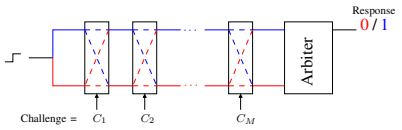

Figure 1. Arbiter PUF structure

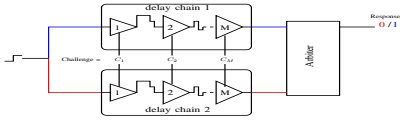

Figure 2. Impoved arbiter PUF structure.

B. *Loop PUF*

Even with the design proposed by majzoobi et al. [3], the arbiter PUF still needs routing constraints before and after the delay chains. In order to avoid these constraints, Cherif et al. [2] have proposed the loop PUF. The latter is composed of N delay chains implemented sequentially forming a loop. When closed by an inverter, this loop oscillates as a single ring oscillator (Figure 3).

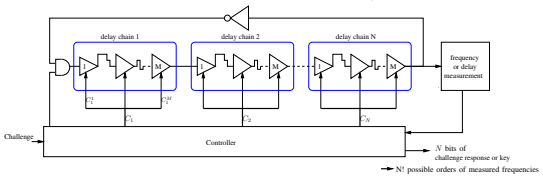

Figure 3. Loop PUF structure.

III. Design and performance comparison

A. *Mixed PUF design: PUFmix*

In order to make a fair performance comparison, we use the same delay chains on the arbiter and loop PUF structures. Figure 4 shows the PUFmix structure designed on both Xilinx and ASIC platforms. In order to evaluate the uniqueness of the response of each structure, we designed 49 identical PUFmix on the two platforms. With the PUFmix design we make 3 independent PUFs:

- Arbiter PUF #1 (uses the two upper delay chains).
- Arbiter PUF #2 (uses the two bottom delay chains).
- Loop PUF (uses the four delay chains).

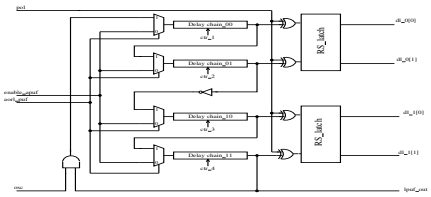

Figure 4. PUFmix design

B. *ASIC vs FPGA, loop vs arbiter PUF*

For intra-device evaluation process, we use the method proposed by Hori et al. in [4] that is based on statistical studies of binary outputs of PUFs. The best values of randomness, steadiness and uniqueness are those closed to 100%.

Figure 5 and 6 show the average of intra-device evaluation results of the 49 arbiter PUF #1 and the 49 arbiter PUF #2, respectively. On FPGA, the randomness of the arbiter PUF #1 is 0%. This means that there is a bias between the two parallel paths due to imperfect routing. The bit response of the PUF is stable (always at '0' or '1') even when changing the control word. The intra-device evaluation of the arbiter PUF #2 shows that the bias on FPGAs is reduced and the randomness of the arbiter PUF #2 increases to 25%. However, on ASIC, the two arbiter PUFs present the same performance results. Then, we can conclude that, due to manual routing, the design in ASIC is slightly better in terms of randomness (around 25%). Since there is a bias on the design of the arbiter PUF structures, we can not judge the steadiness witch is around 100% on both platforms. The two platforms are built with the CMOS 65nm technology, due to the noise of designed and unused components on the FPGA, the extraction process is better on ASIC. This makes the uniqueness of the designed PUFs better on ASIC than FPGA.

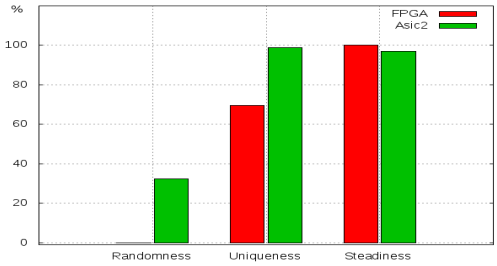

Figure 5. Arbiter PUF #1 intra-device evaluation

Figure 6. Arbiter PUF #2 intra-device evaluation

The average intra-device evaluation of the loop PUF structure shows that the loop PUF is better than the arbiter PUF (Figure 7). Since there is no routing constraints, the loop PUF presents a good randomness on both platforms (around 100%). Also, the steadiness of the loop PUF is around 100%. Due to imperfect extraction of the CMOS variation on FPGAs, the intra-device uniqueness of the loop PUF is better on ASIC. We can conclude that the loop PUF design is better than the arbiter PUF on both CMOS 65nm platforms ASIC and FPGA.

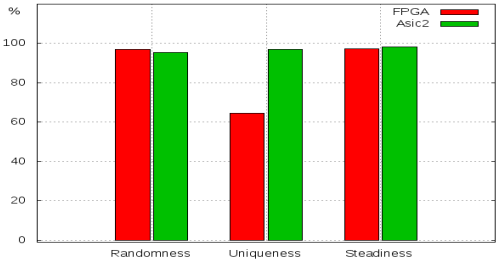

Figure 7. Loop PUF intra-device evaluation

IV. Conclusion

We have compared the performance of the arbiter and the loop PUFs designed on two platforms with CMOS 65nm technology. Using the same delay chains, the loop PUF is more efficient than the arbiter PUF in terms of randomness. The arbiter PUF has a best performance characteristics on ASIC due to manual routing. The loop PUF presents good randomness on both platforms since there is no need for routing constraints. On the CMOS 65nm technology, the extraction of CMOS variation is better on ASIC than FPGA which allows a better uniqueness of PUFs.

Acknowledgement: This work was supported by Orange Labs and the Frech Telecom Institute and the European project ENIAC ("Toise").

References

[1] Blaise Gassend, Dwaine E. Clarke, Marten van Dijk, and Srinivas Devadas. Silicon physical random functions. In *ACM Conference on Computer and Communications Security*, pages 148–160, 2002.

[2] Zouha Cherif Jouini, Jean-Luc Danger, Sylvain Guilley, and Lilian Bossuet. An easy to design puf based on a single oscillator: the loop puf. DSD'12, 2012.

[3] M. Majzoobi, F. Koushanfar, and S. Devadas. FPGA PUF using programmable delay lines. In *Information Forensics and Security (WIFS), 2010 IEEE International Workshop on*, pages 1 –6, December 2010.

[4] Yohei Hori, Takahiro Yoshida, Toshihiro Katashita, and Akashi Satoh. Quantitative and statistical performance evaluation of arbiter physical unclonable functions on fpgas. *Reconfigurable Computing and FPGAs, International Conference on*, 0:298–303, 2010.